# Dissertation Title

Enda O’Shea

Dissertation 2017

Erasmus Mundus MSc in Dependable Software Systems



Department of Computer Science,

Maynooth University,

Co. Kildare, Ireland.

A dissertation submitted in partial fulfilment

of the requirements for the

Erasmus Mundus MSc Dependable Software Systems

Head of Department : Dr Adam Winstanley

Supervisor : Dr Rosemary Monahan

15-June-2018

Word Count: 0000

Contents

[Declaration i](#_Toc447110597)

[Acknowledgements ii](#_Toc447110598)

[Abstract iii](#_Toc447110599)

[List of Figures iv](#_Toc447110600)

[List of Tables iv](#_Toc447110601)

[**Chapter one: Introduction** 1](#_Toc447110602)

[Summary 1](#_Toc447110603)

[1.1 Topic addressed in this project 1](#_Toc447110604)

[1.2 Motivation 1](#_Toc447110605)

[1.3 Problem statement 1](#_Toc447110606)

[1.4 Approach 2](#_Toc447110607)

[1.5 Metrics 2](#_Toc447110608)

[1.6 Project 2](#_Toc447110609)

[**Chapter two: Related Work** 3](#_Toc447110610)

[Summary 3](#_Toc447110611)

[2.1 Topic material 3](#_Toc447110612)

[2.2 Technical material 3](#_Toc447110613)

[**Chapter three: The Problem** 4](#_Toc447110614)

[Summary 4](#_Toc447110615)

[3.1 Project UML documentation 4](#_Toc447110616)

[3.2 Problem analysis 4](#_Toc447110617)

[**Chapter four: The Solution** 6](#_Toc447110618)

[Summary 6](#_Toc447110619)

[Depending on your type of project, you may not need to include all of these: 6](#_Toc447110620)

[4.1 Analytical Work 6](#_Toc447110621)

[4.2 Architectural Level 6](#_Toc447110622)

[4.2 High Level 6](#_Toc447110623)

[E.g. Packages, Class Diagrams, etc. 6](#_Toc447110624)

[4.2 Low Level 6](#_Toc447110625)

[E.g. Method specifications, Algorithms, etc. 6](#_Toc447110626)

[4.2 Implementation 6](#_Toc447110627)

[**Chapter five: Evaluation** 7](#_Toc447110628)

[Summary 7](#_Toc447110629)

[5.1 Solution Verification 7](#_Toc447110630)

[E.g. use your equations to verify the correctness of your solution 7](#_Toc447110631)

[5.2 Software Design Verification 7](#_Toc447110632)

[5.3 Software Verification 7](#_Toc447110633)

[5.3.1 Your test approach (i.e. unit testing, sub-system testing, system testing) 7](#_Toc447110634)

[5.3.2 Your tests (e.g. scenarios, test cases, test data, etc.) 7](#_Toc447110635)

[5.3.3 Your test results 8](#_Toc447110636)

[5.3.4 An interpretation of the results 8](#_Toc447110637)

[5.4 Validation/Measurements 8](#_Toc447110638)

[5.4.1 Results 8](#_Toc447110639)

[5.4.2 Explanation of Results 8](#_Toc447110640)

[5.4.3 Analysis of Results 8](#_Toc447110641)

[5.4.4 Comparison with previous solutions (if relevant) 8](#_Toc447110642)

[**Chapter five: Conclusion** 9](#_Toc447110643)

[**Summary** 9](#_Toc447110644)

[5.1 Contribution to the state-of-the-art 9](#_Toc447110645)

[5.2 Results discussion 9](#_Toc447110646)

[5.3 Project Approach 9](#_Toc447110647)

[5.3 Future Work 9](#_Toc447110648)

[**References** 10](#_Toc447110649)

[**Appendices** 11](#_Toc447110650)

[Appendix 1 Schematic of the hardware associated with this project. 12](#_Toc447110651)

[Appendix 2 Code developed for this project. 13](#_Toc447110652)

[Appendix 3 UML Class, Use Case and sequence diagrams for this project. 14](#_Toc447110653)

[Appendix 4 Screen shots of the project implementation 15](#_Toc447110654)

[Appendix 5 Taught M.Sc. Dissertation Guidelines (valid from Oct 2015) 16](#_Toc447110655)

## Declaration

I hereby certify that this material, which I now submit for assessment on the program of study as part of Master of Science in Dependable Software Systems qualification, is *entirely* my own work and has not been taken from the work of others - save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: Date:

## Acknowledgements

Rosemary Monahan

David R. Cok

## Abstract

Formal specification and software verification of software have become increasingly pertinent in the past decade, as a way of supplementing the already popular software testing techniques, to both improve software quality and provide a more concrete proof of reliability. However, the use of these proof techniques has not been wholly adopted by industry due to business factors such as the time required for specifying the source code and costs related to such a process, to the more technical factors such as the difficulty in specifying and verifying code with the current tools and languages available, with an expert in the domain often required to get valid implementations.

In this project we will be focusing on a verification tool called OpenJML, developed by David R. Cok with Java as its target language, that set out to simplify the development of specifications using the JML language and simplify the verification process using SMT provers, with the overall goal of wide adoption by industry professionals. This project sets out to examine, the updated version of this tool, to see if a novice user can adopt the techniques required to specify and verify pieces of software. We plan to determine OpenJML’s validity as an industry alternative in comparison to similar existing verification tools, and to examine its performance as a standalone specification and verification tool.

**Category, Terms, Keywords: OpenJML, Formal Specification, JML, KeY, Why3, Deductive Verification**

**NB: See Appendix 5 for the official guidelines on how to write this thesis.**

## List of Figures

[Figure 3‑1 UML class diagram overview for this project. 4](#_Toc445718606)

## List of Tables

[Table 2‑1 Table of interest: Aspect of your implementation 2](#_Toc445714278)

[Table 2‑2 Data sources used in your implementation 2](#_Toc445714279)

# **Chapter one: Introduction**

## Summary

Chapter 1 describes….

**Introduction – a high level description of the research question and the problem domain that can be understood by somebody new to the subject area.**

* + **Objectives –** A single sentence that describes the purpose of this section.
  + **Research Question** – State the technical problem that you have focused on in your project in the form of a question which you address.
  + **Motivation** – Discuss the reasons for solving this problem. Detail the problem domain and who would be interested in the solution. Describe the likely impact of your work. Address both why it is an interesting technical problem, and also the value of solving it in more general terms.
  + **Aims and Objectives** – State the aims and objectives of your project. The **aims** of your project are the overall goal, and the **objectives** are the stepping stones in reaching that goal. Identifying the objectives helps the reader to understand your overall project approach.
  + **Report Structure** - Outline the structure of the report summarizing each chapter in one sentence.

## 1.1 Overview

Formal specification and software verification of software have become increasingly pertinent in the past decade, as a way of supplementing the already popular software testing techniques, to both improve software quality and provide a more concrete proof of reliability. This lead to the Programming by Contract approach that was popularised by Bertrand Meyer (*Meyer, B. 1992*) , however was presented in earlier works (Insert Works?), with the overall goal being to reduce defensive programming and increase reliability by introducing mathematical proofs into a methods specification, therefore enforcing the clients and suppliers compliance (InsertQuote?).

However, the use of these proof techniques has not been wholly adopted by industry due to business factors such as the time required for specifying the source code and costs related to such a process, to the more technical factors such as the difficulty in specifying and verifying code with the current tools and languages available, with an expert in the domain often required to get valid implementations.

## 1.2 Motivation

‘VerifyThis’ (Pm.inf.ethz.ch. (2018) is a program verification competition that requires contestants to specify and verify a certain number of tasks within a certain time limit, usually 45 minutes per question. The winners of these competitions in the past five years, 2018 included, were teams that used the verification tools Isabelle, Why3, KIV, Verifast with KeY and Dafny also proving popular. These tools, with the exception perhaps of Dafny, are non-intuitive by nature and require vast amounts of expertise and skill to master with no regular cross-over functionality between them or interface to connect them (Source).

The developers of these tools do not communicate regularly (Source) with each other and focus primarily of developing their own tool’s functionality. This lack of co-ordination has led to many different tools that, even though proven to work, are not adopted by many users outside of their field. Novice users, just coming into the formal verification domain, especially have a steep learning curve with separate libraries and syntax variables to conquer while trying to embrace the core concepts of Programming by Contract. This lack of co-operation and co-ordination has increased the delay of verification being adopted outside of academia with industry primarily focused on developing software products in a timely, cost effective matter. Ensuring reliability is paramount to all software development projects, however the time and expertise required for integrating one of the verification tools above seems to be too much for industry to handle and relies primarily on the proven but not fully sound software testing techniques (Source).

OpenJML aims to bridge this gap (Source) by allowing its freely available tool to be integrated into the Eclipse IDE directly and using only the popular JML specification language with sequential Java programs. A command-line tool is also available and the overall goal of the tool is simplicity for novice and expert users alike. This project aims to evaluate how easy in fact it is to use this tool in comparison to its competitors, KeY also has an Eclipse plugin, and if the stripping down to just the basics of JML with Java would actually be viable for real-life industrial systems.

## 1.3 Problem statement

Describe the technical problem needed to be solved in your project. Note that most projects solve both a more abstract, high-level problem and a specific, technical problem: your problem statement is the detailed technical problem (your motivation should cover the more abstract high-level problem).

## 1.4 Approach

Summarise how you addressed solving the problem.

Provide an overview of how you analysed the problem, how you designed a solution, and how you evaluated your solution. (e.g. use of models, simulation, prototypes, real-world experiments, cases studies, etc.). What important variables did you control, ignore, or measure in your evaluation.

## 1.5 Metrics

Describe how you are going to evaluate your work.

## 1.6 Project

List, and briefly describe your significant achievements in the project (probably 3-5 of these in a typical project). If you have come up with any contributions

# **Chapter two: Related Work**

## Summary

The purpose of this chapter is to show your depth and breadth of reading and understanding of the problem domain

**Related Work – Details what others have done that is relevant to your work.**

* + **Objectives –** A single sentence that describes the purpose of this section.
  + Describe the context of the research question in detail, defining terminology, and with references.
  + Explain how the problem, or related problems, has been solved previously. Critically analyze existing solutions. Discuss how your approach compares to these solutions.
  + Explain other techniques that you have used to: help understand and analyze the research question; motivate your own work; evaluate your solution.

## 2.1 Topic material

(Research material, if used, from published journals and conference proceedings; less academic publications, if required by the project, from other sources) – for example, what other work researchers have done already in this area, what results they have produced, what work has been done in related areas, what software already exists to solve this or similar problems, etc.

## 2.2 Technical material

(From any source: including books, websites) – for example, how to write a web server, how to use specific Java features, how to use Ajax, how to use UML to validate your design, etc.

NB: Note that material relating to the motivation or non-technical background should **NOT** go here, but rather in the introduction

Table 2‑1 Table of interest: Aspect of your implementation

|  |  |
| --- | --- |
| **Column description 1** | **Column description 2** |
| A | Text 1 |
| B | Text 2 |
| C | Text 3 |

Table 2‑2 Data sources used in your implementation

|  |  |  |
| --- | --- | --- |
| **Column description 1** | **Column description 2** | **Column description 3** |
| X | 22 | 33 |
| Y | 33 | 456 |
| Z | 17 | 22 |

# **Chapter three: The Problem**

## Summary

The purpose of this chapter is to clearly explain the technical problem and/or identify the user requirements.

## 3.1 Project UML documentation

Provide any model(s) of the problem (e.g. equations, ERD’s, UML Use Cases & Scenarios, Activity Diagrams, etc.)



Figure 3‑1 UML class diagram overview for this project.

## 3.2 Problem analysis

Provide any analysis of the problem, leading to a greater understanding

There should be no decisions made in this chapter

# **Chapter four: The Solution**

## Summary

The purpose of this chapter is to clearly identify, discuss, and justify the decisions you made.

“**Solution” (often the name of your solution) – Details what you have done and how you have done it.**

* + **Objectives –** A single sentence that describes the purpose of this section.
  + Provide an analysis of the problem, motivating your approach to answering the research question.
  + Explain your approach by describing exactly what you have done.
  + Explain how you have achieved your solution. Examples: explain how a process improvement was implemented, how a mathematical technique was derived, or how an algorithm was implemented.

## Depending on your type of project, you may not need to include all of these:

## 4.1 Analytical Work

E.g. Equations, etc. that describe your solution

## 4.2 Architectural Level

E.g. Implementation Diagrams

## 4.2 High Level

## E.g. Packages, Class Diagrams, etc.

## 4.2 Low Level

## E.g. Method specifications, Algorithms, etc.

## 4.2 Implementation

Discuss anything interesting here; put full source code in an appendix or attachment

# **Chapter five: Evaluation**

## Summary

Chapter 5 describes……..

**Evaluation – Evaluates your work (both in absolute terms, and compared to other solutions)**

* + **Objectives –** A single sentence that describes the purpose of this section.
  + Explain what was evaluated or validated.
  + Experimental setup – Detail how you evaluated and validated your work.
  + Present your results clearly and objectively, without interpretation - ideally with graphs (data)
  + Explain your results - ideally with explanatory text (analysis) to both explain the meaning of these results, and provide the reasons for why these particular results were obtained
  + Critically analyze your results. Identify the contents in which your results are relevant and any threats are to the validity of your results. Show how well you have answered the research question.
  + Critically analyze your results with respect to the “Related Work” presented earlier.

## 5.1 Solution Verification

## E.g. use your equations to verify the correctness of your solution

## 5.2 Software Design Verification

How did you show that your design worked properly?

Using a model of your solution. E.g. use UML interaction diagrams to verify each scenario.

## 5.3 Software Verification

How did you demonstrate your software worked properly?

If you have not tested your software, then you cannot rely on your results. Clearly describe:

### 5.3.1 Your test approach (i.e. unit testing, sub-system testing, system testing)

### 5.3.2 Your tests (e.g. scenarios, test cases, test data, etc.)

### 5.3.3 Your test results

### 5.3.4 An interpretation of the results

## 5.4 Validation/Measurements

How did you measure how well your solution solved the problem.

### 5.4.1 Results

### 5.4.2 Explanation of Results

### 5.4.3 Analysis of Results

### 5.4.4 Comparison with previous solutions (if relevant)

**Chapter five: Conclusion**

**Summary**

Chapter 5 identifies and discuss the implications of your work.

**Draws conclusions and identifies potential future work**

* + **Objectives –** A single sentence that describes the purpose of this section.
  + Summarize your results. Provide your conclusions (limitations & recommendations) based on the results obtained. Detail the implications of your results with respect to the wider community.
  + Assess how well you have met your project goals. Identify the contributions made by this work.
  + Critically analyze your approach to solving the research question by explaining what was effective in your approach, and what you could have been improved upon.
  + Present possible future work - How could you/others build on your research to advance it further?

5.1 Contribution to the state-of-the-art

If you made a contribution to the state-of-the-art, clearly identify it here.

5.2 Results discussion

Discuss whether your results are general, potentially generalizable, or specific to a particular case. Identify threats to the validity of your results (e.g. limitations, risks introduced by your approach, etc.)

5.3 Project Approach

Discuss your project approach

5.3 Future Work

Discuss future work, based on what you have done (and not done)

# **References**

* *Meyer, B. (1992), "Applying 'design by contract'", Computer, vol. 25, no. 10, pp. 40-51*

#### Pm.inf.ethz.ch. (2018). VerifyThis Competition. [online] Available at: http://www.pm.inf.ethz.ch/research/verifythis.html [Accessed 13 May 2018].

#### **Shonan.nii.ac.jp. (2018). [online] Available at: http://shonan.nii.ac.jp/shonan/wp-content/uploads/2011/09/No.2013-3.pdf [Accessed 13 May 2018].**

* Giorgetti, A., Groslambert, J., Julliand, J. & Kouchnarenko, O. (2008), "Verification of class liveness properties with Java modelling language", *IET Software,*vol. 2, no. 6, pp. 500-514.
* Poll, E. (2009), "Teaching Program Specification and Verification Using JML and ESC/Java2", *Teaching Formal Methods : Second International Conference, TFM 2009, Eindhoven, The Netherlands, November 2-6, 2009. Proceedings,*vol. 5846, pp. 92-104.

#### **Eecs.ucf.edu. (2018). The Java Modeling Language (JML) Home Page. [online] Available at: http://www.eecs.ucf.edu/~leavens/JML//index.shtml [Accessed 13 May 2018].**

#### **Why3.lri.fr. (2018). Why3 . [online] Available at: http://why3.lri.fr/ [Accessed 13 May 2018].**

#### **Key-project.org. (2018). The KeY Project. [online] Available at: https://www.key-project.org/ [Accessed 13 May 2018].**

Leavens, G.T., & Cheon, Y. (2003). Design by Contract with JML.

Cok, D.R., Leavens, G.T., & Ulbrich, M. (2018), Java Modelling Language Reference Manual

#### **Eecs.ucf.edu. (2018). JML Reference Manual: JML Reference Manual. [online] Available at: http://www.eecs.ucf.edu/~leavens/JML/jmlrefman/jmlrefman.html [Accessed 13 May 2018].**

* Leavens, G.T., Kiniry, J.R. & Poll, E. 2007, "A JML Tutorial: Modular Specification and Verification of Functional Behavior for Java" in Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 37-37.

#### **Cs.ru.nl. (2018). Talks . [online] Available at: https://www.cs.ru.nl/E.Poll/talks/ [Accessed 13 May 2018].**

* Kiniry, J., Morkan, A. & Denby, B. 2006, "Soundness and completeness warnings in ESC/Java2", ACM, , pp. 19.

#### **Kindsoftware.com. (2018). [online] Available at: http://kindsoftware.com/documents/talks/KSU\_ESCJava2\_Object\_Logic.pdf [Accessed 13 May 2018].**

* Cok, D.R. & Kiniry, J.R. 2005, "ESC/Java2: Uniting ESC/Java and JML: Progress and Issues in Building and Using ESC/Java2, Including a Case Study Involving the Use of the Tool to Verify Portions of an Internet Voting Tally System" in Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 108-128.

**Appendices**

Include here all extra material, e.g. your source code, project management (optional) including: the task list, Gantt Chart diagrams (or equivalent), discussion of any significant deviations from plan, and how you managed them, discussion of what you would do differently if you repeated the project.

## Appendix 1 Schematic of the hardware associated with this project.

## Appendix 2 Code developed for this project.

## Appendix 3 UML Class, Use Case and sequence diagrams for this project.

|  |
| --- |
|  |
| Appendix 4 Screen shots of the project implementation |
|  |

## Appendix 5 Taught M.Sc. Dissertation Guidelines (valid from Oct 2015)

**Taught M.Sc. Dissertation Guidelines**

**(valid from October, 2015)**

This document provides guidelines for your M.Sc. level dissertation for modules CS640 and CS645. There is no standard layout (except for the cover page), as the details may be determined by the project topic and the approach you have taken. You should read a number of other dissertations (available on Moodle or from ePrints) to get an idea of the accepted norms. Your supervisor will be able to advise you further.

Your dissertation won't necessarily be *organised* as shown here, but it MUST *contain* the following information:

* Title
* Abstract
* Introduction
* Related Work
* “Solution” (i.e. title of your work)
* Evaluation
* Conclusions
* References
* Appendices

How you present the research question and your solution will depend to a certain extent on the nature of your project. You need to show that you are aware of other research in the area, and show the relationship of at least one other publication to your own work.

The dissertation absolute limit is 22,000 words (using size 12 Times New Roman font and single line spacing, and not including the appendices). A suggested format for your report is detailed on the next page. Supporting documentation such as your documented code should be uploaded separately as directed by your course co-ordinator. **The submission must be all your own work**. Please read the Maynooth University policy on Plagiarism and ensure that your reference material correctly. The minimum penalty for plagiarism is a failed grade in your thesis.

Recommendation: agree on a “model” report with your supervisor that you can base your approach and layout on. The following diagram shows the ‘flow’ or ‘argument’ you should use in presenting your work.



**Title Page** - Template on next page (replace the highlighted text).

**Abstract -** This is a summary of the research question, your results, and your contribution in 200 words or less.

**Category, Terms, Keywords:** reference [www.**acm**.org/sigs/**publications**/pubform.doc](http://www.acm.org/sigs/publications/pubform.doc)for details

**Suggested sections and sub-sections**

* **Introduction – a high level description of the research question and the problem domain that can be understood by somebody new to the subject area.**
  + **Objectives –** A single sentence that describes the purpose of this section.
  + **Research Question** – State the technical problem that you have focused on in your project in the form of a question which you address.
  + **Motivation** – Discuss the reasons for solving this problem. Detail the problem domain and who would be interested in the solution. Describe the likely impact of your work. Address both why it is an interesting technical problem, and also the value of solving it in more general terms.
  + **Aims and Objectives** – State the aims and objectives of your project. The **aims** of your project are the overall goal, and the **objectives** are the stepping stones in reaching that goal. Identifying the objectives helps the reader to understand your overall project approach.
  + **Report Structure** - Outline the structure of the report summarizing each chapter in one sentence.
* **Related Work – Details what others have done that is relevant to your work.**
  + **Objectives –** A single sentence that describes the purpose of this section.
  + Describe the context of the research question in detail, defining terminology, and with references.
  + Explain how the problem, or related problems, has been solved previously. Critically analyze existing solutions. Discuss how your approach compares to these solutions.
  + Explain other techniques that you have used to: help understand and analyze the research question; motivate your own work; evaluate your solution.
* “**Solution” (often the name of your solution) – Details what you have done and how you have done it.**
  + **Objectives –** A single sentence that describes the purpose of this section.
  + Provide an analysis of the problem, motivating your approach to answering the research question.
  + Explain your approach by describing exactly what you have done.
  + Explain how you have achieved your solution. Examples: explain how a process improvement was implemented, how a mathematical technique was derived, or how an algorithm was implemented.
* **Evaluation – Evaluates your work (both in absolute terms, and compared to other solutions)**
  + **Objectives –** A single sentence that describes the purpose of this section.
  + Explain what was evaluated or validated.
  + Experimental setup – Detail how you evaluated and validated your work.
  + Present your results clearly and objectively, without interpretation - ideally with graphs (data)
  + Explain your results - ideally with explanatory text (analysis) to both explain the meaning of these results, and provide the reasons for why these particular results were obtained
  + Critically analyze your results. Identify the contents in which your results are relevant and any threats are to the validity of your results. Show how well you have answered the research question.
  + Critically analyze your results with respect to the “Related Work” presented earlier.
* **Conclusions – Draws conclusions and identifies potential future work**
  + **Objectives –** A single sentence that describes the purpose of this section.
  + Summarize your results. Provide your conclusions (limitations & recommendations) based on the results obtained. Detail the implications of your results with respect to the wider community.
  + Assess how well you have met your project goals. Identify the contributions made by this work.
  + Critically analyze your approach to solving the research question by explaining what was effective in your approach, and what you could have been improved upon.
  + Present possible future work - How could you/others build on your research to advance it further?

**References –** Proper full complete citations for all referenced documents (NOT a URL). For a master’s level document one would expect up to 30 good references. Use peer-reviewed papers or books: not websites.

**Appendix** – Details of: source code, protocols, data, results, etc.

**Note** – Use a repository to store your code & build procedure.